

## CLAIMS

What is claimed is:

- 1        1. A method of authenticating a user at an un-trusted computing  
2 system, the user having at least one portable computing device coupled to a  
3 peripheral device, the method comprising:
  - 4            randomly generating a temporary password by the portable computing  
5 device;
  - 6            sending the temporary password to the peripheral device;
  - 7            rendering the temporary password by the peripheral device for perception  
8 by the user;
  - 9            inputting a password, by the user, into the un-trusted computing system;
  - 10          receiving, by the portable computing device, the password input by the  
11 user from the un-trusted computing system; and
  - 12          allowing access to the portable computing device using the un-trusted  
13 computing system when the temporary password matches the user-inputted  
14 password.
- 15
- 1        2. The method of claim 1, wherein randomly generating the temporary  
2 password comprises randomly generating the temporary password periodically.
- 3
- 1        3. The method of claim 1, wherein randomly generating the temporary  
2 password comprises randomly generating the temporary password in response  
3 to a user-initiated action to the peripheral device.
- 4
- 1        4. The method of claim 1, wherein the temporary password is valid for  
2 only a predetermined period of time.
- 3
- 1        5. The method of claim 4, wherein the predetermined period of time is  
2 less than one minute.

3

1       6. The method of claim 1, wherein sending the temporary password to  
2 the peripheral device comprises sending the temporary password from the  
3 portable computing device to the peripheral device over a secure wireless link.

4

1       7. The method of claim 1, wherein rendering the temporary password  
2 comprises displaying the temporary password on a display of the peripheral  
3 device.

4

1       8. The method of claim 7, further comprising displaying a number of  
2 seconds until the temporary password expires on a display of the peripheral  
3 device.

4

1       9. The method of claim 1, wherein rendering the temporary password  
2 comprises rendering the temporary password audibly for hearing by the user.

3

1       10. The method of claim 1, wherein the password comprises at least one  
2 of numbers, letters, symbols, images, and shapes.

3

1       11. The method of claim 1, further comprising detecting initiation of an  
2 action by the user to the peripheral device to cause the rendering of the  
3 temporary password.

4

1       12. The method of claim 1, further comprising:  
2           generating an indicator by the portable computing device;  
3           sending the indicator to the peripheral device and the un-trusted  
4 computing system;  
5           rendering the indicator by the peripheral device for perception by the user;  
6           rendering the indicator by the un-trusted computing system for perception  
7 by the user;

8           wherein the user inputs a password only when the indicator rendered by  
9   the peripheral device matches the indicator rendered by the un-trusted  
10 computing system the user desires to use.

11

1           13. The method of claim 1, wherein the peripheral device is at least one  
2 of worn by the user and carried by the user.

3

1           14. The method of claim 1, wherein the portable computing device and  
2 the un-trusted computing system communicate over a wireless link.

3

1           15. An article comprising: a storage medium having a plurality of machine  
2 readable instructions, wherein when the instructions are executed by a  
3 processor, the instructions provide for authenticating a user of an un-trusted  
4 computing system, the user having at least one portable computing device  
5 coupled to a peripheral device, by randomly generating a temporary password by  
6 the portable computing device, by sending the temporary password to the  
7 peripheral device, by receiving at the portable computing device a password  
8 input by the user from the un-trusted computing system, and by allowing access  
9 to the portable computing device using the un-trusted computing system when  
10 the temporary password matches the user-inputted password.

11

1           16. The article of claim 15, wherein instructions for randomly generating  
2 the temporary password comprise instructions for randomly generating the  
3 temporary password periodically.

4

1           17. The article of claim 15, wherein the temporary password is valid for  
2 only a predetermined period of time.

3

1           18. The article of claim 17, wherein the predetermined period of time is  
2 less than one minute.

3

1        19. The article of claim 15, wherein instructions for sending the temporary  
2 password to the peripheral device comprise instructions for sending the  
3 temporary password from the portable computing device to the peripheral device  
4 over a secure wireless link.

5

1        20. The article of claim 15, wherein the password comprises at least one  
2 of numbers, letters, symbols, images, and shapes.

3

1        21. A system for authenticating a user desiring to use an un-trusted  
2 computing system comprising:

3            a portable computing device; and

4            a peripheral device, coupled to the portable computing device, capable of  
5 rendering a password for perception by the user;

6            the portable computing device comprising:

7                a random password generator to randomly generate a temporary  
8 password;

9                a memory to store instructions and data; and

10                a processor to execute the instructions obtained from the memory  
11 to send the temporary password to the peripheral device for rendering to  
12 the user, to receive from the un-trusted computing system a password  
13 input by the user; and to allow access to the data by the un-trusted  
14 computing system when the temporary password matches the user-  
15 inputted password.

16

1        22. The system of claim 21, wherein the peripheral device comprises a  
2 display and renders the password by displaying the password on the display.

3

1        23. The system of claim 21, wherein the portable computing device  
2 communicates with the peripheral device over a secure wireless link.

3

1        24. The system of claim 21, wherein the portable computing device  
2 communicates with the un-trusted computing system over a wireless link.

3

1        25. The system of claim 21, wherein the random password generator  
2 randomly generates the temporary password periodically, the temporary  
3 password valid for only a predetermined period of time.

4

1        26. The system of claim 21, wherein the peripheral device is capable of  
2 being at least one of worn and carried by the user.

3

1        27. The system of claim 21, wherein the peripheral device comprises an  
2 input mechanism activation of which initiates rendering of the password by the  
3 peripheral device.

4

1        28. The system of claim 21, wherein the peripheral device comprises an  
2 input mechanism activation of which causes the portable computing device to  
3 randomly generate a new temporary password.